



Stop.Think.Connect. August 2015 Update

In This Issue

- Back to School: Protecting Students Online
 - Cyberbullying Can Happen to Anyone, At Any Age
 - Resource Spotlight: AARP's "Watch Your Wi-Fi Campaign"
 - Cyber in the News: Connected Car Gets Hacked Remotely
 - Partner Spotlight: Cyberbullying Research Center
-

BACK TO SCHOOL: PROTECTING STUDENTS ONLINE

As summer winds down and kids head back to school, it is important to remember to talk to your kids about cyberbullying before they return to the classroom.

Cyberbullying affects more people than one might realize. Seven in ten young people have experienced online bullying, according to a recent survey by the anti-bullying nonprofit organization, Ditch the Label. Students are leading more digital lives, with computers and tablets becoming increasingly common in classrooms, as well as at home. It is critical that parents and teachers equip students with the knowledge and resources to handle and respond to incidents of online bullying.

The Stop.Think.Connect.™ Campaign encourages all parents and educators to take the following steps to help students be aware of cyberbullying and how to handle bullying online if it occurs.

- Start conversations regularly about practicing online safety.
- Create an open and honest environment with kids so they can feel comfortable coming to you, or a trusted adult, if they see something online that makes them feel uncomfortable.
- Emphasize the concept of credibility to kids: not everything they see on the Internet is true, and people on the Internet may not be who they appear to be.
- Tell children to keep their personal information private, including the names of family members, their school, and their telephone number and address.
- Encourage them to think twice before they post or say anything online. Once it is in cyberspace, it is out there forever.

It's also important to remember that cyberbullying doesn't just affect young children – college students and adults may also face online bullying. Following and sharing these simple cybersecurity tips can help to create a better, safer online atmosphere this school year.

For more information on cyberbullying, please visit the Stop.Think.Connect. Campaign Blog: dhs.gov/stopthinkconnect-campaign-blog

CYBERBULLYING CAN HAPPEN TO ANYONE, AT ANY AGE

As we spend more and more time online, bullying or harassment that previously only occurred face to face now occurs online.

Oftentimes, we associate cyberbullying with younger students in the K-12 age group; however, cyberbullying can happen to anyone at any age. Online harassment including hazing, intimidation, stalking, or other manifestations of interpersonal harm that occur on college campuses or in the workplace also fall into the cyberbullying category.

[The Cyberbullying Research Center](#), a Campaign National Network partner, shared these tips for adults who are victims of cyberbullying:

- **Do not respond.** Cyberbullies want you to react. If you respond angrily, the bully may feed off of that response and continue (and even escalate the severity of) the cyberbullying.
- **Record everything.** Keep evidence of all content (pictures, texts, emails, tweets, status updates, etc.) that the cyberbully has sent or posted about you.
- **Talk about it.** Speaking with trustworthy friends about what you are going through could be cathartic. They might have gone through similar situations and might be able to give you advice.
- **Block the bully.** Block the cyberbullying at its source. If you are getting incessant emails from a cyberbully, use your email program options to prevent that person from contacting you.

For a full list of tips and more information, click [here](#) and visit their website for more tips and information: cyberbullying.us.

RESOURCE SPOTLIGHT: AARP'S "WATCH YOUR WI-FI"

On a free public network or even at home, using Wi-Fi means you're potentially sharing your credit card numbers, passwords, and other personal information with the world, including crooks. With cybercrime costing Americans \$800 million last year, the AARP Fraud Watch Network launched "[Watch Your Wi-Fi](#)" – a new campaign to give you the tools you need to protect yourself from hackers.



To get started, here are four things to never do on a public Wi-Fi:

1. **Mind your business:** Don't access your email, online bank or credit card accounts using public Wi-Fi.
2. **Don't fall for a fake:** Con artists may set up unsecured networks with similar names to a coffee shop, hotel, or other free Wi-Fi network.
3. **Watch your settings:** Don't let your mobile device automatically connect to nearby Wi-Fi.
4. **Stick to your cell:** Don't surf using an unknown public network if the website requires sensitive information — like online shopping. While cell phone networks have their risks

they are safer than public Wi-Fi.

For more information, check out the AARP's new video [here](#) and visit the "Watch Your Wi-Fi" campaign at www.aarp.org/watchyourwifi

CYBER IN THE NEWS: CONNECTED CAR GETS HACKED REMOTELY

Last month, a [Wire.com](#) story about two security researchers who were able to hack, remotely control, and crash a Jeep Cherokee created a lot of buzz across the nation. From miles away, the hackers were able to change the radio station, turn the windshield wipers on, and play with the air conditioning. Chips installed in the car that provide wireless and cellular access presented vulnerabilities that the hackers were able to exploit in order to control the cars from the Internet, no matter their location. In response to the incident, Fiat Chrysler released a free software patch for the vulnerability.

This experiment illustrates a very important point about evolving technology. As more and more of our devices – from cars to refrigerators to medical devices – become connected to the Internet, we must be aware of the risks they present and take steps to protect our devices and ourselves.

Here are some tips to increase the security of your Internet-enabled devices:

1. **Update the software regularly.** Regularly install software updates on the device itself as well as the apps you use to control the device.
2. **Think twice about your device.** Have a solid understanding of how a device works, the nature of its connection to the Internet, and the type of information it stores and transmits.
3. **Secure your network.** Properly secure the wireless network you use to connect Internet-enabled devices.

Check out the Stop.Think.Connect. Campaign's [Internet of Things Tip Card](#) for more information and tips.

For more information about how to protect yourself online, please visit dhs.gov/stopthinkconnect.

PARTNER SPOTLIGHT: CYBERBULLYING RESEARCH CENTER

The [Cyberbullying Research Center](#), a member of the Stop.Think.Connect. National Network, provides resources for parents, educators, law enforcement officers, counselors, and others who work with youth to help prevent and respond to cyberbullying. The organization is dedicated to providing up-to-date information about the nature, causes, and consequences of cyberbullying.

On their website, you'll find an array of resources including:

- A cyberbullying blog with the latest news and information on the topic
- Facts, figures, and detailed stories from those who have been directly impacted by online aggression
- Presentation materials for educators, students, and community members

Visit their website, cyberbullying.us and follow them on Twitter, [@OnlineBullying](#), to learn more.


Let Us Know What You Think.

We want to hear what you think about Stop.Think.Connect.
resources.

Do you find the newsletters helpful and informative? Are there
topics you would like to learn more about?

Did you recently attend a Stop.Think.Connect. event? If you did,
what did you like or not like?

Please share your thoughts with us via stopthinkconnect@dhs.gov.

 SHARE

Update your subscriptions, modify your password or e-mail address, or stop subscriptions at any time on your [Subscriber Preferences Page](#). You will need to use your e-mail address to log in. If you have questions or problems with the subscription service, please contact subscriberhelp.govdelivery.com.

This service is provided to you at no charge by the [U.S. Department of Homeland Security](#).

[Privacy Policy](#) | GovDelivery is providing this information on behalf of U.S. Department of Homeland Security, and may not use the information for any other purposes.



**Homeland
Security**